Assessing the Legality and Proportionality of Communications Surveillance in United States Law

By Mark Rumold, EFF Staff Attorney

March 2016

ELECTRONIC FRONTIER FOUNDATION

Table of Contents

I.

Introduction

While privacy is a core component of United States law, new technologies have raised questions about the circumstances under which U.S. citizens can expect their data to be safe from access by the government. This paper begins an analysis and discussion of U.S. law and surveillance practices, measured against two key principles in the International Principles on the Application of Human Rights to Communications Surveillance.[1] This document of 13 principles was created by legal experts worldwide to clarify how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to Communications Surveillance technologies and techniques. The Principles are firmly rooted in well-established human rights law. In particular, they draw on the rights to privacy, freedom of opinion and expression, and freedom of association as guaranteed in international human rights instruments.

Although this paper does not provide exhaustive coverage of all state and federal laws governing communications surveillance in the United States it does identify and discuss significant themes present in U.S. surveillance law. Specifically, the paper addresses how the U.S. Constitution as well as a range of federal and state laws address the values of Legality and Proportionality outlined in the Necessary and Proportionate Principles.

First, the advent of new technologies has unfortunately created uncertainty surrounding the application of U.S. law to modern surveillance practices. Additionally, some outdated laws and complicated applications of previous laws result in a situation in which U.S. law fails to meet the standards of clarity and precision outlined by the Principle of Legality.

Furthermore, while the Proportionality Principle is reflected on paper in both constitutional law and statutory law, the government's actual use of new surveillance technologies runs contrary to this principle. Again, the result is that violations of the Proportionality Principle are widespread, including in the National Security Agency's bulk collection of data and the powerful broad surveillance tools increasingly used by local law enforcement agencies.

Even as courts struggle to reach a consensus on how aging laws will apply to new surveillance technologies, some state legislatures are innovating to protect the privacy of their citizens. Ultimately, in order to create a unified standard for government access to a

range of different types of electronic data, it may be necessary for the United States Congress to adopt comprehensive communication surveillance reform.

II.

The Legality Principle

The first of the Necessary and Proportionate Principles is "Legality." This principle means that any limitation on the right to privacy must be prescribed by law. Specifically, the State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing, publicly reviewable law which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of its application. As the European Court of Human Rights has explained, "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[2] Thus "legality" requires that laws be clear, non-secret, and subject to oversight, and that such laws not vest governmental officials with excessive discretion.[3]

Generally, domestic U.S. law comes from two sources: (1) federal or state constitutions; and (2) federal or state statutory law. Until recently, both federal and state constitutional and statutory law was lagging far behind technological advancements. As it relates to the Principle of Legality, this situation disadvantaged citizens, who were unable to effectively regulate their conduct or understand with certainty the legal process the government was required to follow before accessing sensitive protected information or conducting electronic surveillance. But in the last several years, courts and legislatures at both the federal and state level have become more engaged in regulating electronic surveillance. Some have even extended privacy protections to citizens in new ways.

A. The Legality Principle in U.S. Law

Constitutional Protections

The most important source of regulation for electronic surveillance is the Fourth Amendment to the United States Constitution, which prohibits the government from engaging in unreasonable searches and seizures. This generally requires law enforcement to obtain a "search warrant" before searching a place, including electronic devices and other

forms of digital data. A "search" under the Fourth Amendment is defined as either (1) a government trespass onto private property for the purpose of obtaining information; or (2) a government intrusion into a place where a person has a subjective expectation of privacy that society would accept as reasonable.[4] The Fourth Amendment is a baseline; states and the federal government are free to provide stronger protection for citizens through legislation or state constitutions.[5]

Because the U.S. Supreme Court—the final arbiter of constitutional law in the United States—only decides a handful of cases each year, the government often relies on older, analog cases to decide questions of modern search and seizure.

For example, in the 1970s, the U.S. Supreme Court ruled police could search items found on individuals, like a pack of cigarettes, without a warrant or individualized suspicion after they were arrested.[6] When cell phones became ubiquitous by the end of the 21st century, the government routinely argued that cell phones were the equivalent of a pack of cigarettes, and they were free to rummage through it at will. Lower courts reached conflicting opinions on the issue, leading to different rules in different parts of the country.[7]

In 2014, the issue was resolved definitively when the U.S. Supreme Court ruled in *Riley v. California*, 134 S.Ct. 2473 (2014) that police were not permitted to search the data on a cell phone of an individual who had been arrested without a warrant. *Riley* rejected as "strained" an attempt to treat a cell phone as equivalent to a physical item like a pack of cigarettes. Instead, the Court conducted an independent analysis of the nature of digital data and found the privacy concerns were great enough to require that police use a warrant. The ruling focused specifically on the fact that digital data was qualitatively and quantitatively different than physical items and found that a rule that allowed the search of a cigarette pack could not be extended to the data on a cell phone.

Riley provides a blueprint for how courts can ensure that surveillance is conducted in a way that meets the Principles' standard for Legality. The decision, which was publicly available, created a clear rule that did not give government officials excessive discretion. Instead, it provided the government with a standardized framework for accessing digital data from individuals arrested—using a search warrant—and put citizens on notice about their privacy rights.

Other courts should follow the lead of *Riley* and create clear rules that the government can easily follow and that citizens can understand.

The *Riley* approach is implicated in other technological tools available to police. For

example, there is currently a vigorous debate in the U.S. about whether police must use a search warrant to obtain historical cell-site information, the cell phone service provider's record of with which tower a particular phone connects. This sensitive data can reveal a person's physical location over an extended period of time, painting an intimate portrait of every place a cell phone owner travels. In the 1970s, the U.S. Supreme Court ruled that there was no right of privacy in records held by third parties, including records of which phone numbers a person dialed.[8] The government has used this analog precedent to argue there is no privacy right in cell phone location records either, even though cell phone location records are far more revealing than the relatively simple phone dialing records reviewed by the Court in the 1970s.

While the U.S. Supreme Court has yet to weigh in on this issue specifically, at least one justice has signaled it is time "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" as "this approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[9] And since 2013, the high courts of three states—Massachusetts, New Jersey, and Florida—have adopted the *Riley* Court's mode of analysis and ruled police need a warrant to obtain historical cell-site location information.[10] Like *Riley*, these courts focused on the quantitative and qualitative nature of the information sought by the government in determining the legal protection that should apply. And they all settled upon a clear rule—requiring a warrant, based on probable cause—rather than an ad hoc, multi-factor test that officers would have difficulty applying in the field and that the public would have difficulty understanding.

Legislative Protections

Within the United States, constitutional protections are just a baseline; legislatures at both the federal and state level are permitted to go further than what the federal Constitution provides and grant even stronger legal protection.

In fact, the U.S. Congress did exactly that in 1986 when it passed the Electronic Communications Privacy Act (ECPA), intending to provide legal protection to electronic data and records generated by electronic devices and stored by service providers. ECPA was a response to the U.S. Supreme Court decisions of the 1970s finding no right of privacy in records held by third parties; Congress decided to legislate privacy protections in the perceived absence of constitutional protection. But since its passage in the 1980s, ECPA has not been reformed to account for modern technology, resulting in gaps in privacy protection.

This is most vividly demonstrated in ECPA's treatment of the contents of electronic communications like emails or text messages. Under ECPA, the government must use a warrant to obtain the contents of electronic communications from a service provider if the message is in electronic storage for 180 days or less.[11] But once a message is in storage for more than 180 days, the law does not make clear that a warrant is required and the government may attempt to obtain messages through lesser process.[12] This 180-day dividing line is a relic of the era: in the 1980s, online storage was small and Congress presumed most people would download their important messages onto their computers—protected by the Fourth Amendment—and any messages still in electronic storage after 6 months were effectively abandoned. Today, people use email quite differently: the advent of cloud computing and smart phones has resulted in people keeping their messages online in order to access them everywhere rather than downloading them onto their computers. Unfortunately, Congress has failed to update ECPA since the 1980s. So even though the way people use email has dramatically changed, the law has failed to keep pace.

At the state level, many states have passed laws providing greater privacy protection than ECPA.[13] Some states have passed laws requiring police use a warrant to obtain the contents of electronic communications—regardless of their time in storage.[14] Other states have passed laws requiring a warrant before police can track a person's location with a cell phone.[15]

Most impressively, in 2015 California passed a comprehensive surveillance reform law. Discarding the patchwork of laws that had previously governed law enforcement access to personal information in California, the new law imposes a single warrant requirement for a variety of different types of protected information. Now, for example, in order to obtain emails, texts, or any private document stored by a third party, the police must obtain a warrant issued by a neutral magistrate. That same warrant requirement applies to information about a person's location and to electronic communication "metadata."[16]

B. Areas of U.S. Law Requiring Further Development of the Legality Principle

The Legality Principle requires public access to laws governing surveillance, but United States' electronic surveillance law is plagued by secrecy. This is true for both national security surveillance and for surveillance conducted for domestic law enforcement purposes. Although numerous Constitutional principles exist in U.S. law to guarantee citizens the right to access and understand the law,[17] these principles are honored more in the breach in the electronic surveillance context.

First, in the national security context, the executive branch regularly invokes its "classification" authority[18] to conceal legal opinions or judicial decisions concerning

surveillance from public disclosure. In 1978, the United States established a specialized court, the Foreign Intelligence Surveillance Court ("FISC"), to hear applications from the government concerning national security surveillance.[19] After the terrorist attacks of September 11, 2001, the government began petitioning the FISC for increasingly aggressive authority to conduct surveillance within the United States. Because the FISC's proceedings were secret and *ex parte*, the government succeeded in convincing the court to authorize a number of legally dubious surveillance programs.[20] And, because of the executive's classification assertions, those legal opinions remained secret until 2013—when the government declassified many FISC decisions in the wake of Edward Snowden's leaks. The USA FREEDOM Act, a national security reform package passed into law in 2015, addressed this problem: the new law requires the government to declassify and release any "significant" legal interpretation of the FISC.[21] Although FISC decisions now must be disclosed, some national security surveillance programs are never authorized by courts and, thus, their legal review (if any exists) remains hidden within the executive branch. Secret legal interpretations authorizing new surveillance techniques are likewise a problem in domestic law enforcement investigations. Typically, prosecutors and law enforcement officials petition trial court or magistrate judges, *ex parte*, to issue orders authorizing surveillance. The government typically requests that these applications remain under seal and not available to the public so that targets of investigations are not alerted to the fact of the investigation. Although seemingly logical, problems arise when: (1) the surveillance applications are never unsealed, and (2) the use of the surveillance technique is not disclosed, even when it contributes to a criminal prosecution.[22] These factors have worked to conceal law enforcement surveillance techniques—like the use of IMSI catchers or government malware—from public scrutiny and legal challenge.

The Legality Principle also requires clarity, and the United States' approach to communications surveillance—taken as a whole—is anything but. As described above, the patchwork of laws governing access to data varies based on, at least, the following factors:

(1) whether it is a state or federal investigation;

(2) whether a state has adopted more protective rules governing access to information;

(3) whether the investigation is done for law enforcement or intelligence purposes;

(4) whether the information sought is considered "content" or "metadata;"

(5) whether the information sought is "stored" or acquired in "real-time;" and

(6) whether the information is kept with a third party.

Any one of those factors, taken individually or in combination, can affect whether a court order is required to access the data and the relevant standard the government must satisfy to access the information.

The piecemeal approach taken within the United States stems from the absence of federal legislative or judicial action creating a clear and consistent nationwide standard. For example, the landmark legislation passed in California applies only to California law enforcement agencies. Other state and federal officials accessing the same information as law enforcement agencies in California may be able to obtain that information under different legal standards and using different legal process. Although calls have been made for a complete overhaul of federal surveillance laws, so far, none have managed to pass through both bodies of the U.S. Congress. Until such a comprehensive approach is taken, the laws governing access to personal information throughout the United States will continue to lack clarity.

III.

The Proportionality Principle

The second Principle addressed here is "Proportionality." Under it, communications surveillance should be regarded as a highly intrusive act that interferes with human rights and threatens the foundations of a democratic society. Decisions about communications surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

This assessment requires a State, at a minimum, to establish:

(1) there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim[23] has been or will be carried out;

(2) there is a high degree of probability that relevant and material evidence of such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought[24];

(3) other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option;

(4) information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged;

(5) any excess information collected will not be retained, but instead will be promptly destroyed or returned;

(6) information will be accessed only by the specified authority and used only for the purpose and duration for which authorization was given; and

(7) that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

Again, within the United States, the Proportionality Principle is traditionally reflected in both constitutional law and statutory law. Indeed, the interests protected by the Proportionality Principle are deeply embedded in federal and state constitutions; and many statutes regulating electronic surveillance implement protections similar to those contemplated by the Principle. However, new surveillance technology and an increase in the volume of data available through communications surveillance have complicated the application of these Principles, resulting in some government surveillance activities that lack Proportionality.

A. The Proportionality Principle in U.S. Law

Constitutional Protections

The touchstone of the Fourth Amendment—as described above, the federal constitutional amendment most relevant to communications surveillance—is "reasonableness."[25] In general, warrantless searches that intrude on a person's reasonable expectation of privacy are presumptively unreasonable and thus prohibited.[26] The warrant requirement ensures the application of many of the protections embodied in the Proportionality Principle.

First, a warrant to conduct a search or seizure can be issued only on a showing of "probable cause."[27] This requires a government official to provide credible information that would allow the reviewing magistrate to conclude that there is a fair probability that the search will yield evidence of a crime.[28] The "probable cause" requirement mimics the protections afforded in the first and second requirements of the Proportionality Principle.

Second, the warrant must describe the things to be searched or seized with "particularity." The particularity requirement prohibits general searches and ensures that the search will be limited in duration and scope.[29] The need for particularity closely mimics the fourth requirement of the Proportionality Principle—that the "information accessed will be confined to that which is relevant and material."

These Fourth Amendment principles have been tested—and stretched—in their application to new methods of surveillance, like cell-site simulators, as well as communications surveillance that sweeps in large amounts of communications data, like the NSA's bulk surveillance programs or law enforcement "cell tower dumps." Thus far, the Supreme Court has not addressed the Fourth Amendment implications of these new forms of communications surveillance, leaving the lower federal courts to initially grapple with the issues. Cell-site simulators (also known as "IMSI Catchers" or "Stingrays") implicate Fourth Amendment "reasonableness" concerns—both because of the large volume of information swept up and because of the sensitivity of the location information obtained through their use.[30] Increasingly, lower federal courts have shown a reluctance to approve the use of cell-site simulators without a warrant based on probable cause.[31] In light of this increasing resistance, the United States Department of Justice recently announced that federal law enforcement agencies would be required to seek a warrant prior to use of a cell-site simulator.[32]

Even before these changes, many state supreme courts already afforded greater clarity—and greater constitutional protection—for location information obtained from a person's cell phone. For example, the Florida Supreme Court (the highest state court in Florida) has

determined that police use of real-time cell-site information without a warrant violates the Fourth Amendment.[33] Similarly, the New Jersey Supreme Court determined that, under New Jersey's state Constitution, warrantless access to historical cell-site information was prohibited.[34]

Similar Fourth Amendment concerns exist concerning "cell tower dumps"—law enforcement acquisition of records for all cell phones that connect with a specific cell phone tower. Some federal judges have concluded that law enforcement attempts to obtain access to cell tower connection records violate the Fourth Amendment.[35] At least one judge has concluded that cell tower dumps constitute "very broad and invasive search[es] affecting likely hundreds of individuals" requiring, at a minimum, a warrant based upon probable cause.[36]

Indeed, some judges have recognized that cell tower dumps and cell-site simulators are so intrusive that a warrant should issue only if it contains additional privacy protections—protections aimed at safeguarding the privacy of innocent parties whose data are swept up in the surveillance.[37] These concerns echo the fifth requirement of the Proportionality Principle concerning the retention of "excess material" and its prompt destruction or return.

Finally, in addressing questions of mass surveillance of Americans' call records, at least one federal judge has concluded that the National Security Agency's program failed to satisfy the tailoring requirements of the Fourth Amendment. As the judge noted:

> *[The NSA's call records surveillance program] is not, as an initial matter, a discrete or targeted incursion. To the contrary, it is a sweeping, and truly astounding program that targets millions of Americans arbitrarily and indiscriminately.*

The failure to apply any discriminating criteria or tailoring of the surveillance—in other words, the absence of Proportionality—rendered the program unconstitutional in the judge's view.[38]

Legislative Protections

The values embodied in the Proportionality Principle are additionally expressed—and given additional reach beyond that afforded by the Constitution—in legislation at the federal and state levels.

One of the United States' earliest laws governing communications surveillance—the Wiretap Act—codifies many values embodied in the Proportionality Principle, and superimposes additional procedures beyond the probable cause required by the federal

Constitution. Among other things, the Wiretap Act requires that government officials demonstrate that (1) they are investigating one of a series of specific, serious crimes; (2) there is probable cause to believe that the surveillance will yield communications about that serious crime; and (3) normal, less intrusive methods have been attempted or would fail, among other requirements.[39]

The Wiretap Act does not govern all communication surveillance within the United States, however. For example, a separate set of laws governs surveillance in the national security context;[40] and the Wiretap Act, and its later amendments, only apply to "real-time" interception of the contents of communications, leaving different statutory protection at the federal level for "stored" communications, like email, or information associated with a communication, like location information or metadata.[41]

In light of those gaps, several states have passed laws affording greater protection for citizens and further restricting communications surveillance. Again, as described above, California's landmark 2015 communications surveillance legislation now requires police to obtain a warrant in order to obtain a person's location information and to obtain some forms of metadata associated with electronic communications. Other states—like Utah[42] Virginia,[43] and Minnesota[44]—have passed laws requiring a warrant before law enforcement may access location information.

B. Areas of U.S. Law Requiring Further Development of the Proportionality Principle

Despite the protections described above, the Proportionality Principle is not uniformly adhered to throughout U.S. law. Violations of the principle frequently occur in surveillance involving communications "metadata"—like the NSA's practice of collecting call records in bulk or law enforcement attempts to obtain "tower dumps." Although courts, like those described above, are beginning to recognize the sensitivity of metadata collection—especially when that collection occurs in bulk—those courts remain in the minority. The majority of courts still view metadata collection—even in bulk—as unworthy of constitutional protection. The legal theories animating bulk metadata collection exploit the differing level of protections afforded communications "content" and "metadata" under U.S. law. Under controlling Supreme Court precedent from the 1970s, described supra, individuals do not have Fourth Amendment interests in the collection of at least some quantity of records stored with third parties.[45] Based on that precedent, however, some courts have incorrectly concluded that there can never be a constitutionally recognized interest in communications metadata. As the Foreign Intelligence Surveillance Court held, in a decision upholding the constitutionality of the NSA's call record collection program:

> *Where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence ex nihilo.*[46]

Such a conclusion plainly violates the Proportionality Principle. Indeed, the "grouping together" of the information of "large number[s]" of people fundamentally alters the sensitivity of the data: what, in isolation, might not be revealing is radically transformed by the very act of "grouping together." Decisions such as these stray from the Fourth Amendment's core "reasonableness" requirements and, as such, violate the Principle of Proportionality.

In the United States, the absence of Proportionality is not limited to surveillance involving metadata. For example, the NSA scans the content of large quantities of international Internet traffic, searching for email addresses or other identifiers of targets of interest.[47] This so-called "about" surveillance is done without particularized warrants or authorization from a court and results in a search of millions of innocent, untargeted citizen's Internet traffic.

Again, stricter adherence to the Fourth Amendment's touchstone—"reasonableness" would prohibit this type of surveillance. But such sweepingly broad surveillance plainly lacks Proportionality.

IV.
Recommendations

- Courts should require that opinions authorizing new surveillance techniques or raising novel questions of law and technology are made publicly available as soon as possible. If disclosure of the specific opinion is not possible because of national security or law enforcement concerns, then a non-sensitive summary should be prepared and released that informs the public of the nature of the legal dispute and court's conclusions.
- Using California's comprehensive surveillance reform as a model, federal or state surveillance reform must not create arbitrary distinctions between types of protected information, such as the distinctions that currently exist between "content" and "metadata," or "stored" and "real-time" communications. Instead, access to protected information must be predicated on an order issued by a neutral magistrate based on probable cause.
- That reform must also include protection for location data, such as information collected by cell-site simulators, and ensure this data is not collected without an order based on probable cause issued by a neutral magistrate.
- Courts should recognize and enforce the Fourth Amendment's fundamental "reasonableness" requirement and thus prohibit government attempts to collect or analyze protected information in bulk or other ways that effectively eliminate the ability to engage in private communication.

1 https://necessaryandproportionate.org/

2 Judgment in The Sunday Times v. The United Kingdom, Application no. 6538/74, Judgment of 26 April 1979, para .49.

3 Siver v. the UK, Petra v. Romania, 1998. The Human Rights Committee takes the same approach. General Comment No. 34, CCPR/C/GC/34, 12 September 2011, paras. 24 – 26, available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f34&Lang=en

4 Kyllo v. United States, 533 U.S. 27, 33 (2001); Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); United States v. Jones, 132 S. Ct. 945, 949 (2012).

5 Pruneyard Shopping Center v. Robins, 447 U.S. 74, 81 (1980) ("[The federal government does not] limit the authority of the State to exercise its police power or its sovereign right to adopt in its own Constitution individual liberties more expansive than those conferred by the [f]ederal Constitution."). See generally O'Connor v. Johnson, 287 N.W.2d 400, 405 (Minn. 1979) ("The states may, as the United States Supreme Court has often recognized, afford their citizens greater protection than the safeguards guaranteed in the Federal Constitution. Indeed, the states are 'independently responsible for safeguarding the rights of their citizens.'")

6 United States v. Robinson, 414 U.S. 218, 234-35 (1973).

7 Compare United States v. Flores-Lopez, 670 F.3d 803, 805-10 (7th Cir. 2012) (police can search cell phone to obtain its number incident to arrest); People v. Diaz, 51 Cal.4th 84, 101, 244 P.3d 501, 511 (2011) (same) with Smallwood v. State, 113 So.3d 724, 738 (Fla. 2013); State v. Smith, 124 Ohio St. 3d 163, 171, 920 N.E.2d 949, 956 (2009) (police cannot search cell phone incident to arrest).

8 Smith v. Maryland, 442 U.S. 735 (1979).

9 United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring).

10 Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014); State v. Earls, 70 A.3d 630 (N.J. 2013); Tracey v. State, 152 So.3d 504 (Fla. 2014).

11 18 U.S.C. 2703(a).

12 *See* 18 U.S.C. 2703(b), (c).

13 The federal courts, too, have imposed additional protections, beyond those afforded by ECPA. For example, the Sixth Circuit Court of Appeals, in an influential decision, determined that the Fourth Amendment protects emails held by a third-party provider, regardless of the time those emails have been in storage. *United States v. Warshack*, 631 F.3d 266 (6th Cir. 2010).

14 Haw. Rev. Stat. 803-47.6; 16 M.R.S.A. § 642; Texas Code of Criminal Procedure 18.21; Utah Code Ann. § 77-23b-4(a).

15 See Colo. Rev. Stat. Ann. § 16-3-303.5(2); 16 Maine Rev. Stat. Ann. § 648; Minn. Stat. Ann. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Utah Code Ann. § 77-23c-102(1)(a). Six states have passed laws requiring police to obtain a search warrant to track a cell phone in real time. See, Ind. Code § 35-33-5-12; Wis. Stat. Ann. § 968.373(2); 725 ILCS 168/10; Md. Code, Criminal Procedure 1-203.1; Va. Code Ann. 19.2-56.2; HB 1440, amending Wash. Rev. Code 9.73.260 on May 11, 2015.

16 https://www.eff.org/deeplinks/2015/10/victory-california-gov-brown-signs-calecpa-requiring-police-get-warrant-accessing

17 *See, e.g.*, *Papachristou v. Jacksonville*, 405 U.S. 156, 162 (1972) ("Living under a rule of law entails various suppositions, one of which is that '(all persons) are entitled to be informed as to what the State commands or forbids.'"); *Banks v. Manchester*, 128 U.S. 244, 253 (1888) (Judicial opinions constitute "the authentic exposition and interpretation of the law, which, binding every citizen, [are] free for publication to all[.]"); *Sheppard v. Maxwell*, 384 U.S. 333, 349 (1966) ("The principle that justice cannot survive behind walls of silence has long been reflected in the 'Anglo-American distrust for secret trials.'").

18 *See* Executive Order 13526 (governing classification of national security information)

19 *See* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.* (establishing FISC and requiring court orders for foreign intelligence surveillance).

20 *See* Walter F. Mondale, Robert A. Stein, Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 14, 34 (January 1, 2016), Minnesota Law Review, Forthcoming (noting FISC had become "more of a rubber stamp" than a check on executive overreach).

21 The law also authorizes the government to provide a declassified summary of any significant FISC decision, if declassification of the opinion itself proves impossible.

22 This technique, known as parallel construction, works to shield criminal defendants from ever learning that a particular surveillance technique was used in their case. This, in turn, insulates the use of the technique and the orders on which it was based from legal challenge. *See, e.g.*, John Shiffman & Kristina Cooke, *U.S. Direct Agents to Cover Up Program Used to Investigate Americans*, Reuters, *available at* http://www.reuters.com/article/us-deasod-idUSBRE97409R20130805

23 A "Legitimate Aim," for purposes of the principles is one that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. *See* https://en.necessaryandproportionate.org/ ("Legitimate Aim").

24 The 13 Principles has defined protected information as any "information that includes, reflects, arises from, or is about a person's communications and that is not readily available and easily accessible to the general public. Traditionally, the invasiveness of Communications Surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content," "subscriber information" or "metadata," stored data or in transit data, data held in the home or in the possession of a third party service provider.7 However, these distinctions are no longer appropriate for measuring the degree of the intrusion that Communications Surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications—metadata and other forms of non-content data—may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time,8 or of all people in a given location, including around a public demonstration or other political event. As a result, all Protected Information should be given the highest protection in law."

25 Ohio v. Robinette, 519 U.S. 33 (1996).

26 Katz v. United States, 389 U.S. 347, 353 (1967).

27 Illinois v. Gates, 462 U.S. 213, 232 (1983).

28 Id.

29 United States v. Berger, 388 U.S. 41, 56 (1967) (invalidating wiretapping statute that lacked particularity because "need for particularity . . . is especially great in the case of eavesdropping").

30 United States v. In the Matter of the Application of the United States, 15-M-0021 (W.D. Ill. 2015) at 7.

31 *See, e.g.*, In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 2012 WL 2120492 (S.D. Tex. 2012).

32 *See* Justice Department Announces Enhanced Policy for Cell-Site Simulators (Sept. 2015), *available at* http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.

33 Tracy v. Florida, 11-224 (Fla. S. Ct. 2014). Although it was not clear that the police used a cell-site simulator to obtain the real-time location information in this case, the holding would apply in such a situation.

34 New Jersey v. Earls, 70 A.3d 630 (N.J. 2013).

35 In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info, 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011) ("The advent of technology collecting cell-site-location records has made continuous surveillance of a vast portion of the American populace possible: a level of Governmental intrusion previously inconceivable.").

36 In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d), 930 F. Supp. 2d 698 (S.D. Tex. 2012).

37 *See* id. at 702 ("Although the use of a court-sanctioned cell tower dump invariably leads to such information being provided to the Government, in order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information."); *see also* United States v. In the Matter of the Application of the United States, *supra* at 27 ("[T]he Court believes that a process must be created to reasonably ensure that innocent third parties' information collected by the use of a cell-site simulator is not retained by the United States or any government body.")

38 Klayman v. NSA, 957 F. Supp. 2d 1 (D.D.C. Nov. 2015).

39 18 U.S.C. § 2518(3).

40 *See generally,* the Foreign Intelligence Surveillance Act, codified at 50 U.S.C. ch. 36.

41 The Stored Communications Act, 18 U.S.C. §§ 2701-27012.

42 http://le.utah.gov/~2014/bills/static/HB0128.html

43 https://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+HB1408ER

44 https://www.revisor.mn.gov/statutes/?id=626A.42

45 Smith v. Maryland, 442 U.S. 735 (1979).

46 https://fas.org/irp/agency/doj/fisa/fisc-082913.pdf.

47 *See, e.g.*, Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, at 7, 35-37 (July 2, 2014) (describing upstream and "about" surveillance).